2

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-039156

(43)Date of publication of application : 12.02.1999

(51)Int.Cl. G06F 9/06
G06F 12/14
G06F 12/14
G09C 1/00

(21)Application number : 09-195451

(22)Date of filing : 22.07.1997

(71)Applicant : FUJI XEROX CO LTD

(72)Inventor : SASAKI SHIGEHIKO

(54) ENCIPHERED DATA DECODING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent encipherment-protected data from being illegally used due to an altered decoding support program.

SOLUTION: Receiving a decoding instructiona decoding device 100 temporarily stops operation of a CPU. An address detection part 103 monitors memory accessing of the CPU and acquires a store address Pr of an instruction code that issues the decoding instruction. A cipher authentication part 102 authenticates a cipher key. A decoding support program authentication part 104 acquires the authentication range designation (prepost) from the cipher keycalculates a message summary number using a unidirectional hash function about an area covering Pr-pre through Pr+postand compares the calculation result with the message summary number contained in the cipher key to authenticate the correctness of the decoding support program. When this authentication succeedsa data decoding part 101 acquires a cipher decoding key from the cipher key and decodes the enciphered data.

CLAIMS

[Claim(s)]

[Claim 1]An encryption data decoding device comprising:

encryption data decoding device **** which decodes data which was mounted in computer systems and enciphered -- a data decryption means to decode enciphered data based on an encryption key.

An encryption key authentication means which attests that the above-mentioned encryption key is just.
An address detection means to detect a memory address of an instruction code which issued the above-mentioned decoding directions in a decoding support program when decoding directions receive from CPU.
A decoding support program authentication means which attests that the above-mentioned decoding support program is just based on a memory address of the above-mentioned instruction code.

[Claim 2]The encryption data decoding device according to claim 1 which has further an unlawful access prevention means which detects it and takes confrontation measures when a flow of processing is unjustly taken by interruption etc. during execution of the above-mentioned decoding support program.
[Claim 3]The encryption data decoding device according to claim 1 or 2 which verifies whether the above-mentioned decoding support program authentication means has the genuine contents of the code of a predetermined memory address range determined by memory address of the above-mentioned instruction code.
[Claim 4]The encryption data decoding device according to claim 3 which verifies that the contents of the code of the above-mentioned predetermined memory address range are genuine based on a calculation result by a predetermined function of the contents of the code of the above-mentioned predetermined memory address range.
[Claim 5]It is the predetermined encryption data decoding device according to claim 4 made into a tropism function on the other hand about the above-mentioned predetermined function.
[Claim 6]The encryption data decoding device according to claim 4 or 5 with which the above-mentioned encryption key holds a reference value generated from a genuine decoding support programcompares a calculation result by the above-mentioned decoding support program verifying means with the above-mentioned calculation result which the above-mentioned encryption key holdsand the justification of the above-mentioned decoding support program is attested.
[Claim 7]The encryption data decoding device according to claim 6 generated based on a memory address range as which the above-mentioned encryption key held further information which specifies the above-mentioned predetermined memory address rangeand the above-mentioned reference value was specified.
[Claim 8]An encryption data decoding device comprising:
encryption data decoding device **** which decodes data which was mounted in computer systems and enciphered -- a data decryption means to decode enciphered data based on an encryption key.
An address detection means to detect a memory address of an instruction code which transmitted the above-mentioned predetermined information in a decoding support program to the above-mentioned bus when predetermined information is

transmitted to a bus from CPU.
A decoding support program authentication means which attests that the above-mentioned decoding support program is just based on the contents of the above-mentioned decoding support program of a predetermined memory address range determined by memory address of the above-mentioned instruction code.

[Claim 9]An encryption key information generating device which generates encryption key informationcomprising:
A main part of an encryption key which decodes encryption data.
A calculation result by a predetermined function of a code of the predetermined range of a decoding support program used in order to decode the above-mentioned encryption data.
A signature to the above-mentioned main part of an enciphering keyand the above-mentioned calculation result.

[Claim 10]A decoding support program verification method comprising:
A main part of an encryption key which decodes encryption data.
A calculation result by a predetermined function of a code of the predetermined range of a decoding support program used in order to decode the above-mentioned encryption data.
A step which receives encryption key information including a signature to the above-mentioned main part of an enciphering keyand the above-mentioned calculation result.
A step which takes out a code developed by memory area corresponding to the above-mentioned predetermined range of a decoding support program used for decoding when decoding encryption dataA step which compares a step which generates a calculation result by the above-mentioned predetermined function of a code by which picking appearance was carried out [above-mentioned]and the generated above-mentioned calculation result with the above-mentioned calculation result in the above-mentioned encryption key informationand a step which verifies Shinsei of a decoding support program used for the above-mentioned decoding based on a result of the above-mentioned comparison.

[Claim 11]Computer systems comprising:
A bus.
CPU connected to the above-mentioned bus.
A memory connected to the above-mentioned bus.
Have the authentication device connected to the above-mentioned busand the above-mentioned authentication deviceWhen decoding directions of encryption data are transmitted via the above-mentioned bus from the above-mentioned CPUAn address detection means to detect a memory address of an instruction code which issued the above-mentioned decoding directions in a decoding support programand an

authentication means which attests that the above-mentioned decoding support program is just based on a memory address of the above-mentioned instruction code.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application]This invention relates to the art which decodes the enciphered data.
[0002]
[Description of the Prior Art]When applying a cipher system to computer systems and decoding and using conventionally the program and data which were encipheredit is common to execute the decoding program (program which supports decoding calculation and it) which operates on the system (JP3-68024A). By the wayin the open computer systems with which specification was exhibitedSince the analysis and change of a program are easyby changing the decoding support portion (henceforth a decoding support program) of a decoding programUsing decoded data unjustly against the specification of the original decoding program was completed simplyand the safety of the whole system had the problem of becoming low. Progress of a coincidence method is remarkable and many cipher systems with powerful encryption strength are proposed. Howeverthe problem by the analysis of a decoding program and change is unsolvablehowever it may adopt a cipher system with high intensity in order not to be dependent on the safety of the cipher system currently used.
[0003]As a proposal which is going to solve this problemthe decoding program itself is enciphereda decoding program is decoded only at the time of data decryptiona means to do data decryption work is adoptedandtherebywhat makes the analysis and change of a decoding program difficult is known (JP9-6232A). Howeversince decoding a decoding program is also performed by the program after allit does not become essential solution but has only an effect of making some analyses and costs which change takes increase. And since the increasing cost cannot become a serious obstacle if the improved efficiency of a computer in recent years is taken into considerationthere is a problem that the analysis and change of a decoding program cannot be prevented effectively. Once it succeeds in change of a decoding programexecution of an alteration program cannot be prevented but there is a problem that prevention of appropriation of the decoded data to the purpose which is not intended cannot be performed.
[0004]As a result of CPU's supervising the address which accesses a memory and comparing it with the memory access pattern of the just decoding program expected as a means to prevent change of a decoding programwhen it is judged that it is

justpermit memory accessbut. When it is judged that it is inaccuratethere is a proposal which prevents the unjust data use which is not meant by intercepting memory access (JP5-324483A). Howeversince a program exists in the fixed address position if it is the special small system that the program for apparatus inclusion is supplied by ROMjudgment of the justification of a decoding program is possible by supervising the address which CPU accessesbut. In a common systemsince the address with which a program is loaded is determined dynamicallythere is a problem that a decoding program cannot be judged by the address information to access. Since the access pattern of an unjust judging standard cannot be changed easilyit is lacking in extendibility and it difficult to deal with many encryption data. Thereforein common computer systemsthis technique has the problem that it cannot be used.

[0005]In the Prior artin common computer systemsexecution of the decoding program which could not attest that it was a just thing by which the decoding program is not changed at the time of decodingbut was changed as a result in it could be preventedand it twisted and cut as stated above. For this reasonappropriation for the purpose by the decoding program altered and changed which decoded data does not intend cannot be prevented effectively. Thereforethe safety of the whole system has the problem of becoming lowirrespective of the intensity of a cipher system.

[0006]

[Problem(s) to be Solved by the Invention]Also in the open computer systems with which specification was exhibitedthis invention enables it to attest the justification of a decoding program at the time of decoding of encryption dataand makes it the technical problem for this to prevent appropriation of the decoded data to the purpose by the altered decoding program which is not intended.

[0007]

[Means for Solving the Problem]A data decryption means to decode enciphered data based on an encryption key to an encryption data decoding device which decodes data which was mounted in computer systems and enciphered in order to attain the above-mentioned purpose according to this inventionWhen decoding directions think of it from CPU as an encryption key authentication means which attests that the above-mentioned encryption key is justAn address detection means to detect a memory address of an instruction code which issued the above-mentioned decoding directions in a decoding support programHe is trying to establish a decoding support program authentication means which attests that the above-mentioned decoding support program is just based on a memory address of the above-mentioned instruction code.

[0008]In this compositionthe contents of the code of a field appointed beforehand are verified based on a memory address of an instruction code which issued decoding directions in a decoding support programand the justification of a decoding support program can be attested. In this case-izing can be carried out [****] using an address of an instruction code detected even if a decoding support program was

loaded to which field of a memory.
[0009]
[A mode of implementation of an invention] Belowan example of this invention is described with reference to drawings. Drawing 1 shows computer systems which decode encryption data using a decoding device of this invention. In this exampleencryption data is decoded by the decoding device 100 mounted in computer systemsand a decoding support program executed with computer systems.
[0010]In drawing 1CPU202the I/O part 203the decoding device 100and the memory 205 are connected to the internal bus 201and computer systems are constituted. CPU202 is a thing of a general stored program and operates according to directions of a program code which read via the internal bus 201interpreted and read a program code stored in the memory 205. A user of a system can use a system as he means by giving directions by a program so that data stored in the I/O part 203 and the memory 205 via the internal bus 201 CPU202 may be accessed.
[0011]Drawing 2 shows an example of composition of the decoding device 100 of drawing 1. In this figurethe decoding device 100 is constituted including the data decoding section 101the encryption key authentication section 102the address detection part 103the decoding support program authentication section 104and the unlawful access prevention parts 105. The data decoding section 101 decodes enciphered data based on an encryption key. The encryption key authentication section 102 attests that the encryption key 303 (drawing 5) is just. The address detection part 103 detects a memory address of an instruction code which issued the decoding directions in the decoding support program 301 (drawing 3)when directions of decoding receive from CPU202. It attests that the decoding support program authentication section 104 has the just decoding support program 301. When a flow of processing is unjustly taken by interruption etc. during execution of the decoding support program 301the unlawful access prevention parts 105 detect itand take confrontation measures.
[0012]Drawing 3 expresses a data storage situation in a memory when decoding enciphered data. In drawing 3the decoding support program 301 is a program which uses decode data for the decoding device 100 for the purpose which issued instructions and was intended so that the enciphered data 302 may be decoded and it may store in the decode data storing region 304. The encryption key 303 (refer to drawing 5) is key data required in order to decode encryption data. Stored addresses in the memory 205 of the decoding support program 301the enciphered data 302the encryption key 303and the decode data storing region 304 are pckand d.
[0013]Drawing 4 is a key map of a memory stored condition of a decoding support program. In drawing 4from the address p to p_{end} on the memory 205 is a field where the decoding support program 301 is stored. An address with which the decoding directions issue portion 402 which publishes decoding directions is contained in the decoding device 204and this code is stored in the decoding support program 301 is pr.

A block which was before divided from a pre byte and was back divided from a post byte from the address pr of the decoding directions issue portion 402 is the decoding support program verification block 403. The justification of a decoding support program is judged using a message summary number of the decoding support program verification block 403. pre and post are specified with the encryption key 303 (refer to drawing 5).

[0014]Drawing 5 is a lineblock diagram of the encryption key 303. The encryption key 303 is digital data and comprises the decode key 501 of a codethe message summary number 502 of a decoding support programthe verification area range specification 503and the signature 504 of the whole encryption key.

[0015]In [drawing 6 shows an example of composition of an encryption key generating device which generates the encryption key 303and] drawing 6An encryption key generating device is constituted including the verification range specification part 505the decoding support program input part 506the decode key input part 507the message summary number generation part 508the signature generating part 509and the encryption key outputting part 510. The verification range specification part 505 receives the number of bytes pre and post which specify an address of a decoding instruction codeand a verification block. The message summary number generation part 508 generates a message summary number of a decoding support program in the range specified with the verification range specification part 505. The signature generating part 509 generates a signature to a message summary number generated by the number of bytes prepostand the message summary number generation part 508 of a decode key inputted from the decode key input part 507and verification block specification information. The encryption key outputting part 510 makes one pre of a decode keya message summary numberand block specification information and postand a signatureand outputs them.

[0016]Belowdecoding processing of this example is explained. In this examplethe decoding support program 301 and the decoding device 100 perform decoding processing jointly. Drawing 7 is a flow chart of the decoding support program 301. Drawing 8 is a flow chart showing a flow of processing of the decoding device 100. In drawing 7if execution of the decoding support program 301 is started in order to decode encryption datapretreatment will be performed first (Step 601). In pretreatmentthe encryption data 302 and the encryption key 303 are loaded to the memory 205the field 304 which stores decode data is securedand work which constitutes a memory storing situation as shown in drawing 3and other required pretreatments are performed. Nextstored address [of an encryption key] kstored address [of encryption data] cand appointed stored address d of decode data are given to the decoding device 100. It carries out by specifically outputting kcand d to an I/O Address by which the map was carried out to the decoding device 100 through the internal bus 201 (Step 602). Of courseyou may communicate with the decoding device 100 with an option.

[0017]Thendirections are published [performing decoding processing to the decoding device 100and] (Step 603). An address with which an instruction code equivalent to Step 603 is stored at this time is Pr. Issue of these directions is performed by specifically outputting an indication instruction to an I/O Address by which the map was carried out to the decoding device 100 through the internal bus 201.

[0018]The decoding device 100 which decodes can supervise what kind of access CPU202 is carrying out via the internal bus 201. A memory can be accessed directlywithout passing CPU (DMA:Direct Memory Access). In additionoperation of CPU202 is controlledCPU202 can be maintained at a temporary stopped state if neededor operation can be made to resume.

[0019]In drawing 8in Step 701the decoding device 100 which received decoding directions makes operation of CPU202 suspend immediatelyand reads stored address [of the encryption key 303] kstored address [of the encryption data 302] cand appointed stored address d of decode data (Step 701). Therebythe decoding support program 301 will be in a temporary stopped state at Step 603. All accesses to the memory 205 of the following decoding devices 100 use DMA.

[0020]Processing of the decoding device 100 progresses to Step 702. In Step 702stored address Pr of an instruction code of decoding directions issue is acquired by the surveillance of access to the memory 205 of CPU202.

[0021]Nextthe encryption key 303 is attested in Step 703. The signature 504 of the whole encryption key is prepared for the encryption key 303and it is attested by electronic title authentication technology whether it is a just encryption key. A signature authentication key is prepared for a decoding deviceandspecificallyit attests using RSA (Rivest-Shamir-Adelman) public-key-encryption art and message abstract generation art using a one-way hash function. Of courseyou may attest by other methods.

[0022]When attestation goes wrongthe encryption key 303 may be altered. The decoding device 100 considers that the encryption key 303 is not justand progresses to Step 705. In Step 705CPU operation is made to resume and an error code which means in CPU "attestation of an encryption key goes wrong" is returned. An error code is stored in a register which CPU202 can read by specifically accessing an I/O Address by which the map was carried out to the decoding device 100. Of courseyou may communicate with CPU202 with an option. In the decoding support program 301 which resumed operationit judges that an error occurred in branching of Step 605error handling is performed at Step 606and it endswithout decoding.

[0023]When it succeeds in attestation of the encryption key 303 in Step 703processing is advanced to Step 704. In Step 704the verification range specification 503 is acquired from the encryption key 303and a message summary number which used a one-way hash function about a field from Pr-pre to Pr+post is computed.

[0024]Thenin Step 706the message summary number 502 of a verification field of a decoding support program in the encryption key 303 is compared with a message summary number computed at the front step 704. When these are not in agreementthe decoding support program 301 which CPU202 is executing means differing from what a publisher of the encryption key 303 meant. The decoding device 100 is regarded as the decoding support program 301 having been alteredand progresses to Step 707. In Step 707operation of CPU202 is made to resume and an error code which means in CPU "attestation of a decoding support program goes wrong" is returned. An error code is stored in a register which CPU202 can read by specifically accessing an I/O Address by which the map was carried out to the decoding device 100. Of courseyou may communicate with CPU202 with an option. The decoding support program 301 which resumed operation judges that an error occurred in branching of Step 605 of drawing 7performs error handling at Step 606and ends itwithout decoding.

[0025]When it succeeds in attestation of a decoding support program at Step 706 of drawing 8processing is advanced to Step 708. In Step 708the decoding device 100 acquires the decode key 501 of a code from the encryption key 303and performs decoding processing of enciphered data. Specifically from twoa decode key of a codeand a secret key in which a separate thing is prepared for every device of a decoding device. A decode key of block cipherssuch as DES (Data EncryptionStandard)is generateddata enciphered by block cipher decoder by DMA is readand a decoding result is written out to a decode data field by DMA. Of coursethe code/decode system of what kind of method may be used.

[0026]After decoding processing finishesdata followed and decoded is used for Step 709. It can prevent that after use has data decoded for the purpose which is not intended by eliminating decoded data from the memory 205 if needed used.

[0027]By supervising access to the internal bus 201 of CPU202the decoding device 100 can detect operation of taking a flow of processing by unjust interruption etc.while the decoding support program 301 is executed by CPU202. When it is detected that a flow of processing was taken unjustlydecoding work is stopped at once and data decoded by then is also destroyed by DMA. With this functioninterference to operation of a program by hardware interrupt can be eliminatedand safety improves further.

[0028]

[Effect of the Invention]As explained abovethis invention prevents appropriation of the decoded data to the purpose by the altered decoding support program which is not intended by checking the justification of a decoding support program at the time of decoding. Therebythe change-proof nature of a decoding support program can be improvedand the safety of the system corresponding to encryption strength can be obtained.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram showing the composition of the computer systems of the example of this invention.

[Drawing 2]It is a block diagram showing the composition of the decoding device of the above-mentioned example.

[Drawing 3]It is a figure explaining the data storage situation in a memory when decoding the enciphered data.

[Drawing 4]It is a figure which the memory stored condition of a decoding support program shows notionally.

[Drawing 5]It is a figure explaining the composition of an encryption key.

[Drawing 6]It is a block diagram showing the example of composition of the encryption key generating device which generates an encryption key.

[Drawing 7]It is a flow chart explaining operation of a decoding support program.

[Drawing 8]It is a flow chart explaining the flow of processing of a decoding device.

[Description of Notations]

100 Decoding device
101 Data decoding section
102 Address detection part
103 Decoding support program authentication section
104 Unlawful access prevention parts
201 Bus
202 CPU
203 I/O part
205 Memory